Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1-17. (Canceled)

18. (New) A data processing method comprising:

maintaining a database containing a table of data in row and column format, at least a portion of the data being encrypted;

maintaining, separate from the table of data, information for controlling access to a specified proper subset of data in the table; and

controlling access to the specified proper subset of data in the table according to the separately maintained information.

19. (New) The method of claim **18**, wherein controlling access comprises controlling access by a specified user or group of users.

20. (New) The method of claim **18**, wherein controlling access comprises controlling access by a specified program or group of programs.

21. (New) The method of claim **18**, wherein the separately maintained information comprises a separate table inaccessible to a user seeking access to the data.

22. (New) The method of claim **18**, wherein the separately maintained information comprises a separate table inaccessible to a program seeking access to the data.

23. (New) The method of claim 18, wherein controlling access to the specified proper subset of the data comprises using a tamper-resistant hardware module.

24. (New) The method of claim 23, wherein the tamper-resistant hardware module is used to perform a cryptographic operation on the data.

25. (New) The method of claim 23, wherein the tamper-resistant hardware module is used to store at least a portion of the separately maintained information.

26. (New) The method of claim 23, wherein the tamper-resistant hardware module comprises a hardware security module.

27. (New) The method of claim 23, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

28. (New) The method of claim 18, wherein the specified proper subset of data comprises a specified column of data.

29. (New) The method of claim 18, wherein the information for controlling access comprises information used in encrypting or decrypting data in the proper subset of data.

30. (New) The method of claim 29, wherein the information used in encrypting or decrypting data comprises information identifying a way of encrypting or decrypting data in the proper subset of data.

31. (New) The method of claim 18, wherein the information for controlling access comprises information identifying an owner of the proper subset of data.

32. (New) The method of claim 18, wherein the information for controlling access comprises encrypted information.

33. (New) The method of claim 18, further comprising:

receiving a request for access to a particular data element in the table, the particular data element containing encrypted data;

obtaining, from the separately maintained data, cryptographic information associated with a proper subset of data in the table, the proper subset containing the particular data element; and

decrypting the data in the particular data element using the cryptographic information.

34. (New) The method of claim 33, wherein decrypting the data is done using a tamper-resistant hardware module.

35 (New) The method of claim 34, wherein the tamper-resistant hardware module comprises a hardware security module.

36. (New) The method of claim 34, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

37. (New) The method of claim 18, further comprising

receiving a request for access to a particular data element in the table, the particular data element containing encrypted data; and

obtaining, from the separately maintained data, information associated with a proper subset of data in the table, the proper subset containing the particular data element; and

providing decrypted data from the particular data element when the information from the separately maintained data indicates that the request for access to the particular data element is an authorized request.

38. (New) The method of claim 37, further comprising decrypting the data from the particular data element using a tamper-resistant hardware module.

39. (New) The method of claim 38, wherein the tamper-resistant hardware module comprises a hardware security module.

40. (New) The method of claim 38, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

41. (New) A method comprising:

providing a database containing a table having at least two columns of data;

encrypting data in a first column using first cryptographic information;

encrypting data in a second column using second cryptographic information;

storing the first and second cryptographic information outside of the table;

controlling access to data in the first column using the first cryptographic information stored outside of the table; and

controlling access to data in the second column using the second cryptographic information stored outside of the table.

42. (New) The method of claim 41, further comprising storing the first and second cryptographic information in a separate table inaccessible to a user seeking access to the data.

43. (New) The method of claim 41, further comprising storing the first and second cryptographic information in a separate table inaccessible to a program seeking access to the data.

44. (New) The method of claim 41, wherein the first and second cryptographic information are stored, in encrypted form, outside of the table.

45. (New) The method of claim 41, wherein at least a portion of the data is encrypted using a tamper-resistant hardware module.

46. (New) The method of claim 45, wherein the tamper-resistant hardware module comprises a hardware security module.

47. (New) The method of claim 45, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

48. (New) A database management system comprising:

a database containing a table having at least two columns of data, at least one column of data being encrypted; and

information stored outside of the table for controlling access to at least one column of data, the information including cryptographic information associated with the encrypted column of data.

49. (New) The system of claim 48, wherein the information is stored in a separate table inaccessible to a user seeking access to the data.

50. (New) The system of claim 48, wherein the information is stored in a separate table inaccessible to a program seeking access to the data.

51. (New) The system of claim 48, wherein the information is stored in encrypted form.

52. (New) The system of claim 48, further comprising a tamper-resistant hardware module for performing cryptographic operations on the encrypted column of data.

53. (New) The system of claim 52, wherein the tamper-resistant hardware module comprises a hardware security module.

54. (New) The system of claim 52, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

55. (New) A computer-readable medium having encoded thereon software for controlling access to a table of data in a database, the software comprising instructions that, when executed by a computer, cause the computer to

maintain, separate from the table of data, information for controlling access to a specified proper subset of data in the table; and

control access to the data in the proper subset according to the separately maintained information.

56. (New) A data processing method comprising:

maintaining a first set of data as a collection of records having fields, at least a portion of the data being encrypted;

maintaining, separate from the first set of data, information for controlling access to a specified proper subset of the first data; and

controlling access to the specified proper subset of the first set of data according to the separately maintained information.

57. (New) The method of claim 56, wherein controlling access comprises controlling access by a specified user or group of users.

58. (New) The method of claim 56, wherein controlling access comprises controlling access by a specified program or group of programs.

59. (New) The method of claim 56, wherein the separately maintained information comprises information that is inaccessible to a user seeking access to the data.

60. (New) The method of claim 56, wherein the separately maintained information comprises information that is inaccessible to a program seeking access to the data.

61. (New) The method of claim 56, wherein controlling access to the specified proper subset of the data comprising using a tamper-resistant hardware module.

62. (New) The method of claim 61, wherein the tamper-resistant hardware module is used to perform a cryptographic operation on the data.

63. (New) The method of claim 61, wherein the tamper-resistant hardware module is used to store at least a portion of the separately maintained information.

64. (New) The method of claim 61, wherein the tamper-resistant hardware module comprises a hardware security module.

65. (New) The method of claims 61, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

66. (New) The method of claim 56, wherein the specified proper subset of data comprises a specified field of data.

67. (New) The method of claim 56, wherein the information for controlling access comprises information used in encrypting or decrypting data in the proper subset of data.

68. (New) The method of claim 56, wherein the information for controlling access comprises information identifying an owner of the proper subset of data.

69. (New) The method of claim 56, wherein the information for controlling access comprises encrypted information.

70. (New) The method of claim 56, further comprising:

receiving a request for access to a particular data element in the first set of data, the particular data element containing encrypted data;

obtaining, from the separately maintained data, cryptographic information associated with a proper subset of the first set of data, the proper subset containing the particular data element; and

decrypting the data in the particular data element using the cryptographic information.

71. (New) The method of claim 70, wherein decrypting the data is done using a tamper-resistant hardware module.

72. (New) The method of claim 71, wherein the tamper-resistant hardware module comprises a hardware security module.

73. (New) The method of claim 71, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

74. (New) The method of claim 70, wherein the proper subset comprises data in one or more specified fields.

75. (New) The method of claim 56, further comprising

receiving a request for access to a particular data element in the first set of data, the particular data element containing encrypted data; and

obtaining, from the separately maintained data, information associated with a proper subset of data in the first set of data, the proper subset containing the particular data element; and

providing decrypted data from the particular data element when the information from the separately maintained data indicates that the request for access to the particular data element is an authorized request.

76. (New) The method of claim 75, further comprising decrypting the data from the particular data element using a tamper-resistant hardware module.

77. (New) The method of claim 76, wherein the tamper-resistant hardware module comprises a hardware security module.

78. (New) The method of claim 76, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

79. (New) A method comprising:

providing a database containing at least two columns of data;

encrypting data in a first column using first cryptographic information;

encrypting data in a second column using second cryptographic information;

storing the first and second cryptographic information apart from the two columns of data;

controlling access to data in the first column using the first cryptographic information; and

controlling access to data in the second column using the second cryptographic information.

80. (New) The method of claim 79, further comprising storing the first and second cryptographic information in a location that is inaccessible to a user seeking access to the data.

81. (New) The method of claim 79, further comprising storing the first and second cryptographic information in a location that is inaccessible to a program seeking access to the data.

82. (New) The method of claim 79, wherein the first and second cryptographic information are stored, in encrypted form, outside of the first and second column.

83. (New) The method of claim 79, wherein at least a portion of the data is encrypted using a tamper-resistant hardware module.

84. (New) The method of claim 83, wherein the tamper-resistant hardware module comprises a hardware security module.

85. (New) The method of claim 83, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

86. (New) A database management system comprising:

a database containing at least two columns of data, a first column of data being encrypted; and

information stored outside of the first column of data for controlling access to the first column of data, the information including cryptographic information associated with the first column of data.

87. (New) The system of claim 86, where in the information is stored in a location that is inaccessible to a user seeking access to the first column of data.

88. (New) The system of claim 86, where in the information is stored in a location that is inaccessible to a program seeking access to the first column of data.

89. (New) The system of claim 86, wherein the information is stored in encrypted form.

90. (New) The system of claim 86, further comprising a tamper-resistant hardware module for performing cryptographic operations on the first column of data.

91. (New) The system of claim 90, wherein the tamper-resistant hardware module comprises a hardware security module.

92. (New) The system of claim 90, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

93. (New) A computer-readable medium having encoded thereon software for controlling access to data in a database stored in row and column format, the software comprising instructions that, when executed by a computer, cause the computer to

maintain, separate from the data, information for controlling access to a specified proper subset of data; and

control access to the data in the proper subset according to the separately maintained information.